IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

the application of :

Appl. No.	:	09/435,899	Confirmation No. 5856
Applicant	:	P. J. Seger	
Filed	:	11/08/1999	
TC/A.U.	:	2175	
Examiner	:	J. F. Betit	
Docket No.	:	TU999050US1	

Title: WIRELESS SECURITY ACCESS MANAGEMENT FOR A PORTABLE DATA STORAGE CARTRIDGE

DECLARATION UNDER 37 C.F.R. Section 1.132

I, Paul M. Greco, declare and say:

That I am a citizen of the United States of America and I reside at 2791 W. Woodview Crest Drive, Tucson, AZ 85742, USA.

That I am a Senior Programmer at IBM Systems Group, in the field of tape drive microcode development, since April 1996.

That I was previously a Senior Design Engineer at Environmental Systems Products, Inc., in the field of code and systems architecture and development, from August 1990 to April 1996.

That I attended college from 1987 to 1988 at the University of Arizona, located in Tucson, AZ.

That I am knowledgeable in the technology and science of Computer Science and Computer Engineering.

That I have reviewed the present U. S. Patent Application Serial No. 09/435,899, and find that it describes "a portable security system *** which resides in a portable data storage cartridge for managing access to the portable data storage cartridge". (Page 3, lines 13-16) (Emphasis added).

"A programmable computer processor is mounted in the portable data storage cartridge and coupled to [a] wireless interface. *** The computer processor provides a user table comprising at least one unique user identifier for each authorized user, *** and at least one permitted activity the user is authorized to conduct with respect to the data storage media. The user identifier, when combined with a user authentication message from the authorized user in accordance with a predetermined algorithm, authorizes the user." This is accomplished by the "computer processor within the portable data storage cartridge". (Page 4, lines 2-21). The permitted activities may comprise management of access, for example, to "5) add entries to the user table, and 6) change/delete entries to the user table." (Page 5, lines 10-16).

That I have reviewed U. S. Patent No. 5,933,498, Schneck et al., and find that it relates to a data distribution system with authoring in one secure environment, and with distribution into another secure environment. (see column 6, lines 49-50, and Figure 1). The Schneck distribution system comprises a usage control in a static environment dictated by "rules" and is received only by a secure access mechanism within a processor or processing system, and does not provide portability of the access nor management of the rules. (see column 15, lines 19-63).

That I have reviewed U. S. Patent No. 4,941,201, Davis, and find that it relates to an "electronic data storage *** apparatus *** wherein a combination power and data signal is received by a preferably portable *** data storage means ***". (Abstract, lines 1-6).

That there are 4 key differences between the present '899 patent application and Schneck and Davis:

1) Location of the authenticating processor:

In the '899 patent application, the computer processor is "mounted in" the portable data storage cartridge and conducts the authentication of the user. (see Page 4, lines 2-21).

Davis shows a data storage device with CMOS logic that stores and addresses data, without any user authentication. (see column 6, lines 22-59).

Schneck shows a data distribution system where the user access mechanism and the data are external to each other, and the decryption is at the access mechanism, which is in a secure environment of the using processor, not with the data. (see Figures 1 and 5, and column 15, line 19 - column 16, line 38).

Having the computer processor with the portable data in the cartridge makes the authentication of the user totally portable.

2) Use of the user identifier:

In the '899 patent application, the user identifier is a functional enabler of the authorization, when combined with a user authentication message. (see Page 4, lines 7-21).

Davis shows an address-like initialization access code to address a particular memory location of the device, but shows nothing directed to a user identifier. (see column 11, lines 20-61).

Schneck shows a passive use of "a particular user or group or class of users" in a "permission list" of the rules, but shows no user identifier for enabling authorization. (see column 23, line 56 - column 24, line 4).

3) Access to the media:

In the '899 patent application, the authentication is of the user, to gain authorization to conduct at least one permitted activity with respect to the data storage media. (see Page 4, lines 7-21).

Davis shows an address-like initialization access code to address a particular memory location of the device, but shows no user authentication or decryption. (see column 11, lines 20-61).

Schneck shows a data usage control with fixed singular "rules" relative to distribution and use of the data, but does not allow a user to do anything with respect to the media. Rather, the "authoring mechanism" has control over the media, and is in a secure environment, separate from the secure environment of the user. (see column 6, lines 49-50, and column 9, lines 46-59).

4) Access management:

In the '899 patent application, the permitted activities include changes to future access as well as changes to the data. (see Page 5, lines 10-16).

Davis has no ability to manage access.

Schneck shows a distribution system under the control of fixed rules with no ability of the user to change, and is read-only with respect to the data at the media. The user may only make changes to the data in use of the data and not to the original data of the media. (see column 17, lines 35-41, and column 22, line 51 - column 24, line 4, and see Figure 20 and column 33, lines 35-49).

That the undersigned declares further that all statements made herein of his own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patents issuing thereon.

Further declarant saith not.

Date: 12/17/2003 /s/ Paul M. Greco

Paul M. Greco